On the number of rational points on Prym varieties over finite fields

Yves Aubry, Safia Haloui

ON THE NUMBER OF RATIONAL POINTS ON PRYM VARIETIES OVER FINITE FIELDS

YVES AUBRY AND SAFIA HALOUI

Abstract. We give upper and lower bounds for the number of rational points on Prym varieties over finite fields. Moreover, we determine the exact maximum and minimum number of rational points on Prym varieties of dimension 2.

1. Introduction

Prym varieties are abelian varieties which come from unramified double coverings of curves.

Let $\pi : Y \longrightarrow X$ be an unramified covering of degree 2 of smooth absolutely irreducible projective algebraic curves defined over $\mathbb{F}_q$ with $q = p^e$, where p is an odd prime number. Let σ be the non-trivial involution of this covering and σ^* the induced involution on the Jacobian J_Y of Y. The *Prym variety* P_π (we will often drop the subscribe π when it is clear from the context) associated to π is defined as

$$P_\pi = \mathrm{Im}(\sigma^* - id).$$

It is also the connected component of the kernel of $\pi_* : J_Y \longrightarrow J_X$ which contains the origin of J_Y.

It is an abelian subvariety of J_Y isogenous to a direct factor of J_X in J_Y. If X has genus $g + 1 \geq 2$, then Y has genus $2g + 1$ by Riemann-Hurwitz formula, and P_π has dimension g.

Prym varieties coming from unramified double coverings of genus $g + 1$ curves provide a family of principally polarized g-dimensional abelian varieties. Let us denote by $\mathcal{A}_g$ the moduli space of principally polarized abelian varieties of dimension g, by $\mathcal{J}_g$ the Jacobian locus in $\mathcal{A}_g$, by $\mathcal{P}_g$ the subset of $\mathcal{A}_g$ corresponding to Prym varieties, and by $\overline{\mathcal{P}}_g$ its closure, then $\overline{\mathcal{P}}_g$ is an irreducible subvariety of $\mathcal{A}_g$, of dimension $3g$ (for $g \geq 5$), containing $\mathcal{J}_g$; for $g \leq 5$ one has $\overline{\mathcal{P}}_g = \mathcal{A}_g$ (see [3]).

We are interested in the maximum and minimum number of rational points on Prym varieties over finite fields. In [10], Perret proved that if X has genus $g + 1$, $\pi : Y \longrightarrow X$ is a double unramified covering over $\mathbb{F}_q$, and $N(X)$ and $N(Y)$ are the respective numbers of rational points on X and Y, then the number of rational points $\#P(\mathbb{F}_q)$ on the associated Prym variety P satisfies

$$\#P(\mathbb{F}_q) \leq \Big(q + 1 + \frac{N(Y) - N(X)}{g}\Big)^g \tag{1}$$

and

$$\#P(\mathbb{F}_q) \geq \Big(\frac{\sqrt{q}+1}{\sqrt{q}-1}\Big)^{\frac{N(Y)-N(X)}{2\sqrt{q}}-2\delta}(q-1)^g \tag{2}$$

Date: July 12, 2013.

2000 *Mathematics Subject Classification.* 14H40, 14G15, 14K15, 11G10, 11G25.

Key words and phrases. Abelian varieties over finite fields, Prym varieties, Jacobians, number of rational points.

where $\delta = 0$ if $\frac{N(Y)-N(X)}{2\sqrt{q}} + g$ is an even integer, and $\delta = 1$ otherwise (here, we have corrected the value of δ given in [10]).

The aim of this paper is to give some new upper and lower bounds on the number of rational points on Prym varieties over finite fields. In the next section, we recall some methods (from [2]) to estimate the number of rational points on an abelian variety, knowing its trace. We also explain how to derive the Perret's bounds (1) and (2) in this setting.

In Section 3, we study the trace of a Prym variety. The results obtained can be combined with the bounds from Section 2 to obtain new bounds on $\#P(\mathbb{F}_q)$ which require less information on P than the Perret's bounds (namely, they do not require the knowledge of $N(Y)$, and the last one is also independent from $N(X)$).

The last section is devoted to the study of Prym surfaces. The main result is exact formulas for the maximum and the minimum number of points on Prym surfaces.

2. Bounding the number of rational points on an abelian variety depending on its trace

Let A be an abelian variety of dimension g defined over a finite field $\mathbb{F}_q$. The *Weil polynomial* $f_A(t)$ of A is the characteristic polynomial of its Frobenius endomorphism. It is a monic polynomial with integer coefficients and the set of its roots (with multiplicity) consists of couples of conjugated complex numbers of modulus $\sqrt{q}$.

Let $\omega_1, \ldots, \omega_g, \overline{\omega}_1, \ldots, \overline{\omega}_g$ be the roots of $f_A(t)$. For $1 \leq i \leq g$, we set $x_i = -(\omega_i + \overline{\omega}_i)$. We say that A is of *type* $[x_1, \ldots, x_g]$. The *trace* of A is defined to be the trace of its Frobenius endomorphism. We denote by $\tau(A)$ the opposite of the trace of A, more explicitly:

$$\tau(A) = -\sum_{i=1}^{g}(\omega_i + \overline{\omega}_i) = \sum_{i=1}^{g} x_i.$$

This is an integer, and since $|x_i| \leq 2\sqrt{q}$, $i = 1, \ldots, g$, we have $|\tau(A)| \leq 2g\sqrt{q}$.

In the case where our abelian variety is the Jacobian J_X of a smooth projective absolutely irreducible curve $X/\mathbb{F}_q$, its trace can be easily expressed in terms of the number $N(X)$ of rational points on X. Indeed, we have

$$\tau(J_X) = N(X) - (q+1) \tag{3}$$

(it follows from the fact that the numerator of the zeta function of X is the reciprocal polynomial of the Weil polynomial $f_{J_C}(t)$).

Now let P be a Prym variety and $\pi : Y \longrightarrow X$ the associated unramified double covering. The map $\pi_* \times (\sigma^* - id) : J_Y \longrightarrow J_X \times P$ has finite kernel and sends the ℓ^n-torsion points of J_Y on those of $J_X \times P$, for any prime number ℓ distinct from the characteristic of $\mathbb{F}_q$. Then, tensorising the Tate modules by $\mathbb{Q}_\ell$, we get an isomorphism of $\mathbb{Q}_\ell$-vector spaces

$$T_\ell(J_Y) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \longrightarrow T_\ell(J_X \times P) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = T_\ell(J_X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \times T_\ell(P) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

which commutes with the action of the Frobenius. Therefore, we have

$$f_{J_Y}(t) = f_{J_X}(t) f_P(t).$$

It follows that

$$\tau(J_Y) = \tau(J_X) + \tau(P),$$

and using (3), we get

$$\tau(P) = N(Y) - N(X). \tag{4}$$

Let us come back to general abelian varieties. With the same notations as before, we can write

$$f_A(t) = \prod_{i=1}^{g}(t-\omega_i)(t-\overline{\omega}_i) = \prod_{i=1}^{g}(t^2 + x_i t + q).$$

It is wellknown that the number of rational points on A is

$$\#A(\mathbb{F}_q) = f_A(1) = \prod_{i=1}^{g}(q+1+x_i). \tag{5}$$

Since $|x_i| \leq 2\sqrt{q}$, one deduces from (5) the classical *Weil bounds*

$$(q+1-2\sqrt{q})^g \leq \#A(\mathbb{F}_q) \leq (q+1+2\sqrt{q})^g. \tag{6}$$

Now, for $\tau \in [-2g\sqrt{q}; 2g\sqrt{q}]$, define

$$M(\tau) = \left(q+1+\frac{\tau}{g}\right)^g \tag{7}$$

and

$$m(\tau) = (q+1+\tau-2(r(\tau)-s(\tau))\sqrt{q})(q+1+2\sqrt{q})^{r(\tau)}(q+1-2\sqrt{q})^{s(\tau)} \tag{8}$$

where $r(\tau) = \left[\frac{g+\left[\frac{\tau}{2\sqrt{q}}\right]}{2}\right]$ and $s(\tau) = \left[\frac{g-1-\left[\frac{\tau}{2\sqrt{q}}\right]}{2}\right]$ (for a real number x, we denote by $[x]$ its integer part).

We have the following estimation of $\#A(\mathbb{F}_q)$ (see [2] and [1]):

Theorem 1. *If $A/\mathbb{F}_q$ is an abelian variety of dimension g, we have*

$$m(\tau(A)) \leq \#A(\mathbb{F}_q) \leq M(\tau(A)).$$

Notice that in the case of Prym varieties, the upper bound of Theorem 1 together with (4) gives the Perret upper bound (1). The lower bound (2), comes from the fact (proved by Perret in the case of Prym varieties) that for any abelian variety, we have

$$\#A(\mathbb{F}_q) \geq \left(\frac{\sqrt{q}+1}{\sqrt{q}-1}\right)^{\frac{\tau(A)}{2\sqrt{q}}-2\delta}(q-1)^g$$

where $\delta = 0$ if $\frac{\tau(A)}{2\sqrt{q}} + g$ is an even integer and $\delta = 1$ otherwise, which is always less precise than the lower bound from Theorem 1 (for more details, see [2]).

In the next section, we will use Theorem 1 without knowing the value of $\tau(A)$ (but having an estimation). In order to do so, we need some basic results on the functions M and m defined by (7) and (8). These results are summarized in the following proposition:

Proposition 2. *The functions M and m are continuous and increasing on $[-2g\sqrt{q}; 2g\sqrt{q}]$.*

Proof. The function M is obviously continuous, and it is increasing because for $\tau \in [-2g\sqrt{q}; 2g\sqrt{q}]$, $q+1+\tau/g \geq q+1-2\sqrt{q} > 0$.

Now, we focus on m. First, notice that the functions r and s are piecewise constant and therefore m is piecewise an affine function with leading coefficient $(q+1+2\sqrt{q})^{r(\tau)}(q+1-2\sqrt{q})^{s(\tau)} > 0$. Hence, the fact that m is increasing follows from its continuity.

We now prove that m is continuous. Let $k \in \{-g, \dots, g-2\}$ be an integer which has the *same parity* as g, and $\alpha \in [0; 2[$. As $[\alpha] \in \{0, 1\}$ and $g+k$ and $g-k$ are non-negative even integers, we have

$$r(2\sqrt{q}(k+\alpha)) = \left[\frac{g+k+[\alpha]}{2}\right] = \frac{g+k}{2} + \left[\frac{[\alpha]}{2}\right] = \frac{g+k}{2}$$

and

$$s(2\sqrt{q}(k+\alpha)) = \left[\frac{g-1-k-[\alpha]}{2}\right] = \frac{g-k}{2} + \left[\frac{-1-[\alpha]}{2}\right] = \frac{g-k}{2} - 1.$$

In particular, the functions r and s are constant on any interval of the form $[2k\sqrt{q}; 2(k+2)\sqrt{q}[$, where $k \in \{-g, \dots, g-2\}$ has the same parity as g, and thus m is continuous (in fact affine) on these intervals.

It remains to check that

$$\lim_{\substack{\alpha \to 2 \\ \alpha < 2}} m(2\sqrt{q}(k+\alpha)) = m(2\sqrt{q}(k+2)).$$

The previous computations show us that

$$r(2\sqrt{q}(k+\alpha)) - s(2\sqrt{q}(k+\alpha)) = k+1,$$

and thus the first factor in the expression of m is

$$q+1+2\sqrt{q}(k+\alpha) - 2(r(2\sqrt{q}(k+\alpha)) - s(2\sqrt{q}(k+\alpha)))\sqrt{q} = q+1+2\sqrt{q}(\alpha-1).$$

We deduce that

$$m(2\sqrt{q}(k+\alpha)) = (q+1+2\sqrt{q}(\alpha-1))(q+1+2\sqrt{q})^{\frac{g+k}{2}}(q+1-2\sqrt{q})^{\frac{g-k}{2}-1}$$

and as

$$m(2\sqrt{q}(k+2)) = (q+1-2\sqrt{q})(q+1+2\sqrt{q})^{\frac{g+k}{2}+1}(q+1-2\sqrt{q})^{\frac{g-k}{2}-2},$$

we have

$$m(2\sqrt{q}(k+\alpha)) = \frac{(q+1+2\sqrt{q}(\alpha-1))}{(q+1+2\sqrt{q})} m(2\sqrt{q}(k+2)),$$

and the result follows. □

Notice that we have

$$m(-2g\sqrt{q}) = (q+1-2\sqrt{q})^g \quad \text{and} \quad M(2g\sqrt{q}) = (q+1+2\sqrt{q})^g,$$

in particular, the bounds of Theorem 1 are always more precise than the Weil bounds (6) (but require more information on A).

3. On the trace of Prym varieties

As before, let A be an abelian variety defined over $\mathbb{F}_q$ of dimension g, $f_A(t)$ be its Weil polynomial, $\omega_1, \dots, \omega_g, \overline{\omega}_1, \dots, \overline{\omega}_g$ be the complex roots of $f_A(t)$, $x_i = -(\omega_i + \overline{\omega}_i)$, $1 \leq i \leq g$, and

$$\tau(A) = -\sum_{i=1}^{g}(\omega_i + \overline{\omega}_i) = \sum_{i=1}^{g} x_i$$

be the opposite of the trace of A. For $k \geq 1$, we also define $\tau_k(A)$ to be the opposite of the trace of $A \times_{\mathbb{F}_q} \mathbb{F}_{q^k}$, that is,

$$\tau_k(A) = -\sum_{i=1}^{g} (\omega_i^k + \overline{\omega}_i^k)$$

(hence we have $\tau_1(A) = \tau(A)$).

We recall the following classical upper bound for $\tau_2(A)$ (see [7]), which is a direct consequence of the Cauchy-Schwartz Inequality:

$$\tau_2(A) = -\sum_{i=1}^{g} x_i^2 + 2gq \leq -\frac{1}{g}\Big(\sum_{i=1}^{g} x_i\Big)^2 + 2gq = \frac{-\tau(A)^2}{g} + 2gq. \tag{9}$$

Now let P be a Prym variety and $\pi : Y \longrightarrow X$ the associated unramified double covering. We denote by $N_k(X)$ and $N_k(Y)$ the respective numbers of rational points on X and Y over $\mathbb{F}_{q^k}$, $k \geq 1$. The results from Section 2 tell us that

$$N_k(X) = q^k + 1 + \tau_k(J_X)$$

and

$$N_k(Y) = q^k + 1 + \tau_k(J_X) + \tau_k(P) = N_k(X) + \tau_k(P).$$

Remark 3. As π is unramified and of degree 2, the number of rational points on Y must be even (it is twice the number of splitting rational points on X). Of course, this holds for any finite extension of the base field, and therefore, for $k \geq 1$, the $N_k(Y)$ are even, or in other words (recall that q is supposed to be odd), we have

$$\tau_k(P) \equiv \tau_k(J_X) \mod 2.$$

Now, we give estimations of $\tau(P)$ which are independent from Y. We start by the following lemma:

Lemma 4. *With the notations above, we have*

$$0 \leq N(Y) \leq 2N(X) \leq N_2(Y).$$

Proof. The first inequality is obvious. For the second one, use the fact that the image of a rational point is a rational point, and the number of points in the preimage of a point is at most 2. For the third one, if we denote by $B_d(Y)$ the number of points on Y of degree d, we have:

$$N_2(Y) = B_1(Y) + 2B_2(Y).$$

The set $X(\mathbb{F}_q)$ can be partitioned into two subsets: the rational points which are splitting and those which are inert in the covering $Y \longrightarrow X$. Denote respectively their cardinal by s and i, we have $B_1(Y) \geq 2s$ and $B_2(Y) \geq i$. Hence, $N_2(Y) \geq 2s + 2i = 2N(X)$. □

The two first inequalities of Lemma 4 give us immediately the following result, which is stated in [10]:

Proposition 5 (Perret)**.** *We have*

$$|\tau(P)| \leq N(X).$$

Notice that the bound of Proposition 5 is sharp when X has few points (in particular, if X has no rational points, then we get the exact value of τ).

The third inequality of Lemma 4 gives us the following proposition:

Proposition 6. *We have*

$$|\tau(P)| \leq \sqrt{g(q^2-1) - \frac{g(N(X)-q-1)^2}{g+1} - 2g(N(X)-q-1) + 4g^2q}.$$

Proof. We have

$$\begin{aligned} 2(q+1+\tau(J_X)) = 2N_1^X &\leq N_2^Y \\ &= q^2+1+\tau_2(J_X)+\tau_2(P) \\ &\leq q^2+1-\tau(J_X)^2/(g+1)+2(g+1)q-\tau(P)^2/g+2gq, \end{aligned}$$

where the last inequality comes from (9). Rearranging the terms, we find

$$\frac{\tau(P)^2}{g} \leq q^2 - 1 - \frac{\tau(J_X)^2}{g+1} - 2\tau(J_X) + 4gq,$$

and using the fact that $\tau(J_X) = N(X) - q - 1$, the result follows (notice that the second term in the previous inequality is necessarily non-negative). □

Remark 7. The third inequality of Lemma 4 is sharp when X has many points. Indeed, we have

$$2N(X) \leq N_2(Y) \leq 2N_2(X)$$

(the last inequality is just the second inequality of Lemma 4 applied after a quadratic extension of the base field), and according to (9), a curve with many points over $\mathbb{F}_q$ must have few points over $\mathbb{F}_{q^2}$.

Now, recall that we have defined

$$M(\tau) = \left(q+1+\frac{\tau}{g}\right)^g$$

and

$$m(\tau) = (q+1+\tau-2(r(\tau)-s(\tau))\sqrt{q})(q+1+2\sqrt{q})^{r(\tau)}(q+1-2\sqrt{q})^{s(\tau)}$$

where $r(\tau) = \left\lfloor \frac{g+\left\lfloor \frac{\tau}{2\sqrt{q}} \right\rfloor}{2} \right\rfloor$ and $s(\tau) = \left\lfloor \frac{g-1-\left\lfloor \frac{\tau}{2\sqrt{q}} \right\rfloor}{2} \right\rfloor$. Theorem 1 and Proposition 2 give us:

Corollary 8. *We have*

$$m(-N(X)) \leq \#P(\mathbb{F}_q) \leq M(N(X))$$

and

$$m\left(-\varphi(N(X))\right) \leq \#P(\mathbb{F}_q) \leq M\left(\varphi(N(X))\right),$$

where

$$\varphi(N(X)) = \sqrt{g(q^2-1) - \frac{g(N(X)-q-1)^2}{g+1} - 2g(N(X)-q-1) + 4g^2q}.$$

By combining Proposition 5 and Proposition 6, we can eliminate the variable $N(X)$:

Proposition 9. *If $|\tau(P)| \geq q-g$ (for instance, this condition is satisfied when $g \geq q$), then we have*

$$|\tau(P)| \leq \frac{g}{2g+1}\Big(q-g+\sqrt{(q-g)^2+(2g+1)(4gq+q^2+6q+1)}\Big).$$

Proof. The last inequality in the proof of Proposition 6 can be rewritten as

$$\frac{\tau(J_X)^2}{g+1} + 2\tau(J_X) + \frac{\tau(P)^2}{g} - q^2 - 4gq + 1 \leq 0.$$

Considering its first term as a polynomial equation in $\tau(J_X)$ and computing the roots, we find

$$\tau(J_X) \leq -(g+1) + \sqrt{(g+1)(q^2+g+4gq-\frac{\tau(P)^2}{g})}.$$

But Proposition 5 tells us that $\tau(J_X) \geq |\tau(P)| - (q+1)$, and therefore, we have

$$|\tau(P)| + g - q \leq \sqrt{(g+1)(q^2+g+4gq-\frac{\tau(P)^2}{g})}.$$

Under the assumptions of the proposition, the first term of this inequality is non-negative, so we can raise everything to the square. We get

$$\begin{aligned}(|\tau(P)| + g - q)^2 &\leq (g+1)(q^2+g+4gq-\frac{\tau(P)^2}{g}) \\ \tau(P)^2 + 2(g-q)|\tau(P)| + g^2 - 2gq + q^2 &\leq gq^2 + g^2 + 4g^2q - \tau(P)^2 + q^2 + g + 4gq - \frac{\tau(P)^2}{g}\end{aligned}$$

Hence

$$-(2g+1)\tau(P)^2 - 2g(g-q)|\tau(P)| + g^2(4gq+q^2+6q+1) \geq 0.$$

Considering the first term of this last inequality as a polynomial equation in $|\tau(P)|$ and computing the roots, we get the result. □

The bound of Proposition 9 is sharper than the Weil bound $|\tau(P)| \leq 2g\sqrt{q}$ if

$$2g\sqrt{q} \geq \Big(q - g + \sqrt{(q-g)^2 + (2g+1)(4gq+q^2+6q+1)}\Big)g/(2g+1),$$

and as the second member is the greatest root of the polynomial in $|\tau(P)|$ considered at the end of the proof of Proposition 9, and the smallest root must be smaller than $2g\sqrt{q}$, this inequality is equivalent to

$$\begin{aligned}0 &\leq (2g+1)(2g\sqrt{q})^2 + 2g(g-q)2g\sqrt{q} - g^2(4gq+q^2+6q+1) \\ 0 &\leq (2g+1)4q + 4(g-q)\sqrt{q} - 4gq - q^2 - 6q - 1 \\ g &\geq (q^2+4q\sqrt{q}+2q+1)/(4q+4\sqrt{q}) = (q\sqrt{q}+3q-\sqrt{q}+1)/(4\sqrt{q}).\end{aligned}$$

Notice that this last condition is satisfied when $g \geq q$.

Remark 10. According to the results of Ihara [7], the number of rational points of a (smooth, projective, absolutely irreducible) curve of genus $(g+1)$ over $\mathbb{F}_q$ is at most

$$\frac{1}{2}\Big(2q - g + 1 + \sqrt{(8q+1)(g+1)^2 + (4q^2-4q)(g+1)}\Big), \tag{10}$$

so using Proposition 5, we get another bound for $|\tau(P)|$. However, it is easy to check that the quantity (10) is always (for any q and g) greater than the second term of the inequality of Proposition 9.

As in Corollary 8, we can derive some bounds on $\#P(\mathbb{F}_q)$ depending only on g and q:

Theorem 11. *If $g \geq q$, we have*

$$(q+1-2\sqrt{q})^g \leq m\,(-\psi) \leq \#P(\mathbb{F}_q) \leq M\,(\psi) \leq (q+1+2\sqrt{q})^g$$

where

$$\psi = \frac{g}{2g+1}\Big(q-g+\sqrt{(q-g)^2+(2g+1)(4gq+q^2+6q+1)}\Big).$$

4. Prym varieties of dimension 2

For any power of an odd prime q and any integer $g \geq 1$, we define the quantities

$$Prym_q(g) = \max_{\pi} \#P_\pi(\mathbb{F}_q) \quad \text{and} \quad prym_q(g) = \min_{\pi} \#P_\pi(\mathbb{F}_q)$$

where π runs over the set of unramified double coverings of genus $(g+1)$ curves defined over $\mathbb{F}_q$.

Theorem 11 gives us bounds on $Prym_q(g)$ and $prym_q(g)$ when $g \geq q$. Here, we are interested in the case where g is small compared to q. More precisely, the aim of this section is to determine $Prym_q(2)$ and $prym_q(2)$. To do so, we will exhibit maximal and minimal Prym surfaces. It turns out that it is enough to consider Prym varieties associated to coverings of hyperelliptic curves, and in this case, the *Legendre construction* gives us an explicit description of the Prym variety. We start by recalling it; for more details, see [9] and [4].

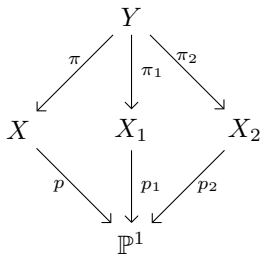
Let X be an hyperelliptic curve of genus g, $p : X \longrightarrow \mathbb{P}^1$ be the associated double covering and $\{z_1, \ldots, z_{2g+2}\}$ be the set of branch points. Then all unramified double coverings $\pi : Y \longrightarrow X$ arise as follows:

(1) Separate the branch points into two nonempty groups of even cardinality: $\{1, 2, \ldots, 2g+2\} = I_1 \cup I_2$, $\#I_1 = 2h+2$, $\#I_2 = 2k+2$, $I_1 \cap I_2 = \emptyset$ (hence $h+k+1 = g$).

(2) Consider the degree 2 maps $p_1 : X_1 \longrightarrow \mathbb{P}^1$ and $p_2 : X_2 \longrightarrow \mathbb{P}^1$ with respective set of branch points $\{z_i\}_{i\in I_1}$ and $\{z_i\}_{i\in I_2}$.

(3) Let Y be the normalization of $X \times_{\mathbb{P}^1} X_1$.

Then, we have such a diagram:



In this situation, the Prym variety P_π associated to the covering $\pi : Y \longrightarrow X$ is isomorphic to the product of the Jacobians of X_1 and X_2:

$$P_\pi \simeq J_{X_1} \times J_{X_2}$$

(the isomorphism is given by $\pi_1^* + \pi_2^* : J_{X_1} \times J_{X_2} \longrightarrow P_\pi$, see [4]).

Moreover, if I_1 and I_2 are chosen to be stable under the action of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ then all the curves and maps involved in this construction will be defined over $\mathbb{F}_q$.

In particular, we have:

Proposition 12. *Let $p_1 : X_1 \longrightarrow \mathbb{P}^1$ and $p_2 : X_2 \longrightarrow \mathbb{P}^1$ be degree 2 maps with disjoints sets of ramified points. Then $J_{X_1} \times J_{X_2}$ is isomorphic to a Prym variety.*

We deduce from Proposition 12 some preliminary results describing when an abelian surface is a Prym variety:

Proposition 13. *A Jacobian of dimension 2 is isomorphic to a Prym variety.*

Proof. A Jacobian of dimension 2 is the Jacobian of a (necessarily hyperelliptic) curve C of genus 2. Let $p : C \longrightarrow \mathbb{P}^1$ the associated double covering. Since C has genus 2, p is ramified at exactly 6 points. Since $\#\mathbb{P}^1(\mathbb{F}_{q^2}) = q^2 + 1 \geq 3^2 + 1 = 10$, there exist unramified points $z_1, z_2 \in \mathbb{P}^1(\mathbb{F}_{q^2})$ such that the set $\{z_1, z_2\}$ is invariant under the action of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ (since the whole set of ramified points is invariant under this action). Now we consider the double covering $p_1 : C_1 \longrightarrow \mathbb{P}^1$ which is ramified at z_1 and z_2 (note that C_1 is a genus zero curve) and we apply Proposition 12. □

Proposition 14. *If E is an elliptic curve defined over $\mathbb{F}_q$ with a rational point z_0 of order strictly greater than 2 then the elliptic curve $\varphi_{z_0}(E)$ where*

$$\begin{array}{rccc} \varphi_{z_0} & : & E & \longrightarrow & E \\ & & z & \longmapsto & z + z_0 \end{array}$$

is isogenous to E, defined over $\mathbb{F}_q$ and has a set of ramified points disjoint from the one of E.

In particular, the product $E \times \varphi_{z_0}(E)$ is isomorphic to a Prym variety.

Proof. The translation by a rational point of order strictly greater than 2 sends the points of order 2 of E on points of order strictly greater than 2. Hence Proposition 12 gives the result. □

These two last propositions are sufficient to prove Theorem 17 (giving the value of $Prym_q(2)$) and most cases of Theorem 18 (giving the value of $prym_q(2)$). In order to deal with the remaining cases of Theorem 18 (namely $q = 3, 5, 9$), we will use the following result:

Lemma 15. *If $\#E(\mathbb{F}_q) = 1, 2$ or 4, then $E \times E$ is isogenous to a Prym variety.*

Proof. Let $p : E \longrightarrow \mathbb{P}^1$ be a double covering defined over $\mathbb{F}_q$ and let $\{z_1, \ldots, z_4\}$ be the branch points. In the light of Proposition 12, it is enough to prove the existence of an automorphism $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ defined over $\mathbb{F}_q$ which sends $\{z_1, \ldots, z_4\}$ on a set disjoint with itself. In the remaining of the proof, we identify $\mathbb{P}^1(\bar{\mathbb{F}}_q)$ with $\bar{\mathbb{F}}_q \cup \{\infty\}$ in the usual way.

• Suppose that $\#E(\mathbb{F}_q) = 1$. Applying to $\mathbb{P}^1$ some suitable rational automorphism, we can assume that $z_1 = 0$. The other branch points are of the form $z_i = \alpha_i$ where the set $\{\alpha_2, \alpha_3, \alpha_4\}$ is contained in $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and invariant under the action of $\mathrm{Gal}(\mathbb{F}_{q^3}/\mathbb{F}_q)$. Consider the map $\varphi : x \mapsto 1/x$. If $\{i, j, k\} = \{2, 3, 4\}$, then on one hand, $\alpha_i \neq -1, 1$, so $\alpha_i \neq 1/\alpha_i$ and on the other hand, we have $\alpha_i \neq 1/\alpha_j$ since otherwise the symmetric product $\alpha_1\alpha_2\alpha_3$ would be α_k, which is not an element of $\mathbb{F}_q$. Therefore, the set of branch points and its image $\{\infty, 1/\alpha_2, 1/\alpha_3, 1/\alpha_4\}$ are disjoint and φ satisfies the required conditions.

• Suppose that $\#E(\mathbb{F}_q) = 2$. If $q = 3$, then by [6], $E \times E$ is isogenous to a Jacobian, so suppose that $q \geq 5$. The elliptic curve E has 2 rational branch points, so applying to $\mathbb{P}^1$ some suitable rational automorphism, we can assume that $z_1 = 0$ and $z_2 = 1$. The other branch points are of the form $z_i = \alpha_i$ where the set $\{\alpha_3, \alpha_4\}$ is contained in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and invariant under the action of $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$. If $c \in \mathbb{F}_q$ then for $\{i, j\} = \{3, 4\}$, we have $\alpha_j \neq \alpha_i + c$, since otherwise the symmetric sum

$\alpha_3 + \alpha_4$ would be $2\alpha_i + c$, which is not an element of $\mathbb{F}_q$. Therefore, we can take φ to be the translation by any element of $\mathbb{F}_q \setminus \{-1, 0, 1\}$ (which exists since $q \geq 5$).

• Suppose that $\#E(\mathbb{F}_q) = 4$. First, writing $\#E(\mathbb{F}_q) = q + 1 + \tau$, we have $|\tau| = |4 - (q+1)| \leq 2\sqrt{q}$, which is possible if and only if $q \leq 9$. In [11], Rück gives a list of the possible group structures for an elliptic curve. Applying his results, we find that if $q \leq 7$, then the group structure $\mathbb{Z}/4\mathbb{Z}$ is possible. Therefore, in these cases, we can choose an element in the isogeny class of E which has a 4-torsion point and apply Proposition 14.

Now suppose that $q = 9$. According to [11], the group $E(\mathbb{F}_9)$ must be isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Therefore, $\{z_1, \ldots, z_4\} \subseteq \mathbb{P}^1(\mathbb{F}_9)$. Applying to $\mathbb{P}^1$ some suitable rational automorphism, we can assume that $\{z_1, z_2, z_3\} = \{-1, 0, 1\}$. In the same way, we can also assume that $z_4 \in \{\infty, c\}$, where $c^2 = -1$. Indeed, if $z_4 \neq \infty$, then $z_4 \in \mathbb{F}_9 \setminus \mathbb{F}_3 = \{\pm d, \pm d \pm 1\}$ with $d^2 = -1$, therefore, possibly applying a translation by ± 1 to $\mathbb{P}^1$ (notice that $\{z_1, z_2, z_3\} = \{-1, 0, 1\}$ is invariant by such a translation), we get what we want.

Consider the map $\varphi : x \mapsto (c+1)(x+c)/(x-c)$. We find that $\varphi(-1) = -(c-1)$, $\varphi(0) = -(c+1)$, $\varphi(1) = c-1$, $\varphi(\infty) = c+1$ and $\varphi(c) = \infty$. Therefore, $\{z_1, z_2, z_3, z_4\}$ and $\{\varphi(z_1), \varphi(z_2), \varphi(z_3), \varphi(z_4)\}$ are disjoint and φ satisfies the required conditions. □

Remark that the proof of Proposition 13 can be easily adapted to prove that Prym varieties of dimension 1 correspond to elliptic curves. Therefore, the values of $Prym_q(1)$ and $prym_q(1)$ can be directly derived from the Deuring-Waterhouse Theorem (see [5], [13]): set $m = [2\sqrt{q}]$ and recall that $q = p^e$ with p an odd prime number; we have:

Proposition 16.

(1) *$Prym_q(1)$ is equal to*
   - *$(q + 1 + m)$ if $e = 1$, e is even or $p \not| m$*
   - *$(q + m)$ otherwise.*

(2) *$prym_q(1)$ is equal to*
   - *$(q + 1 - m)$ if $e = 1$, e is even or $p \not| m$*
   - *$(q + 2 - m)$ otherwise.*

Now, we focus on Prym surfaces. Les us first recall some basic facts about abelian surfaces. Let A be an abelian surface over $\mathbb{F}_q$ of type $[x_1, x_2]$. Its characteristic polynomial has the form

$$f_A(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2,$$

with

$$a_1 = x_1 + x_2 \quad \text{and} \quad a_2 = x_1 x_2 + 2q.$$

By elementary computations, Rück [12] showed that the fact that the roots of $f_A(t)$ are q-Weil numbers (i.e. algebraic integers such that their images under every complex embedding have absolute value $q^{1/2}$) is equivalent to

$$|a_1| \leq 2m \quad \text{and} \quad 2|a_1|q^{1/2} - 2q \leq a_2 \leq \frac{a_1^2}{4} + 2q \tag{11}$$

where $m = [2\sqrt{q}]$. We have

$$\#A(\mathbb{F}_q) = f_A(1) = q^2 + 1 + (q+1)a_1 + a_2. \tag{12}$$

As described in [2], Table 1 gives all the possibilities for (a_1, a_2) such that $a_1 \geq 2m - 2$. The numbers of points are classified in decreasing order and an abelian

variety with (a_1, a_2) not in the table has a number of points strictly less than the values of the table. Here

$$\varphi_1 = (-1+\sqrt{5})/2, \quad \varphi_2 = (-1-\sqrt{5})/2.$$

a_1	a_2	Type	$\#A(\mathbb{F}_q)$
$2m$	m^2+2q	$[m,m]$	b^2
$2m-1$	m^2-m+2q	$[m,m-1]$	$b(b-1)$
	$m^2-m-1+2q$	$[m+\varphi_1, m+\varphi_2]$	b^2-b-1
$2m-2$	$m^2-2m+1+2q$	$[m-1,m-1]$	$(b-1)^2$
	$m^2-2m+2q$	$[m,m-2]$	$b(b-2)$
	$m^2-2m-1+2q$	$[m-1+\sqrt{2}, m-1-\sqrt{2}]$	$(b-1)^2-2$
	$m^2-2m-2+2q$	$[m-1+\sqrt{3}, m-1-\sqrt{3}]$	$(b-1)^2-3$

TABLE 1. Couples (a_1, a_2) maximizing $\#A(\mathbb{F}_q)$ $(b = q+1+m)$.

In the same way, we build the table of couples (a_1, a_2) with $a_1 \leq -2m+2$. If $q > 5$, the numbers of points are classified in increasing order and an abelian variety with (a_1, a_2) not in the following table has a number of points strictly greater than the values of the table (see [2]).

a_1	a_2	Type	$A(\mathbb{F}_q)$
$-2m$	m^2+2q	$[-m,-m]$	b'^2
$-2m+1$	$m^2-m-1+2q$	$[-m-\varphi_1, -m-\varphi_2]$	$b'^2+b'-1$
	m^2-m+2q	$[-m,-m+1]$	$b'(b'+1)$
$-2m+2$	$m^2-2m-2+2q$	$[-m+1+\sqrt{3}, -m+1-\sqrt{3}]$	$(b'+1)^2-3$
	$m^2-2m-1+2q$	$[-m+1+\sqrt{2}, -m+1-\sqrt{2}]$	$(b'+1)^2-2$
	$m^2-2m+2q$	$[-m,-m+2]$	$b'(b'+2)$
	$m^2-2m+1+2q$	$[-m+1,-m+1]$	$(b'+1)^2$

TABLE 2. Couples (a_1, a_2) minimizing $\#A(\mathbb{F}_q)$ $(q > 5$ and $b' = q+1-m)$.

Theorem 17 and 18 will be proved in the following way:

(1) Look at the highest row of Table 1 or 2 (depending on the theorem being proved).
(2) Check if the corresponding polynomial is the characteristic polynomial of an abelian variety.
(3) When it is the case, check if this abelian variety is isogenous to a Prym variety.
(4) When it is not the case, look at the next row and come back to the second step.

For the second step, we use the results of Rück [12] (completed by Maisner, Nart and Xing) describing set of characteristic polynomials of abelian surfaces. More precisely, we use two facts: first, a simple abelian surface with a reducible characteristic polynomial must have trace 0 or $\pm 2\sqrt{q}$, and thus, excluding these two cases if x_1, x_2 are integers, there exists an abelian surface of type $[x_1, x_2]$ if and only if there exists two elliptic curves of respective trace x_1 and x_2 (and in this case, the corresponding isogeny class contains the product of these elliptic curves). Secondly, if (a_1, a_2) satisfy (11) and p does not divide a_2 then the corresponding polynomial is the characteristic polynomial of an abelian surface.

For the third step, we use Proposition 13 combined with results from [6] (which gives a description of the set of isogeny classes of abelian surfaces containing a Jacobian), Proposition 14 and Lemma 15.

Note that this method is still valid for $q \leq 5$, even if Table 2 is not correct anymore. Indeed, we always have $prym_q(2) \geq (q+1-m)^2$ and for $q \leq 5$ there exists a Prym surface with $(q+1-m)^2$ points (the conditions of the first point of Theorem 18 are satisfied for $q = 3, 5$).

Finally, remark that we need to have $|x_i| \leq 2\sqrt{q}$, $i = 1, 2$, thus

- in order to have the existence of an abelian surface with $(x_1, x_2) = \pm(m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2})$, it is necessary that $m + \frac{-1+\sqrt{5}}{2} \leq 2\sqrt{q}$, which is equivalent to $\{2\sqrt{q}\} = 2\sqrt{q} - m \geq \frac{\sqrt{5}-1}{2} \simeq 0,61803$ (where $\{x\}$ denotes the fractional part of x i.e. $\{x\} = x - [x]$),
- in order to have the existence of an abelian surface with $(x_1, x_2) = \pm(-m + 1 + \sqrt{2}, -m + 1 - \sqrt{2})$, it is necessary that $\{2\sqrt{q}\} \geq \sqrt{2} - 1 \simeq 0,41421$,
- in order to have the existence of an abelian surface with $(x_1, x_2) = \pm(-m + 1 + \sqrt{3}, -m + 1 - \sqrt{3})$, it is necessary that $\{2\sqrt{q}\} \geq \sqrt{3} - 1 \simeq 0,73205$.

Theorem 17. *If $q = p^e$, then $Prym_q(2)$ is equal to*

- $(q+1+m)^2$ *if* $e = 1$ *or* e *even or* $p \not| m$
- $(q+1+m-\frac{1+\sqrt{5}}{2})(q+1+m-\frac{1-\sqrt{5}}{2})$ *if* $e \neq 1$, e *odd,* $p|m$ *and* $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$
- $(q+m)^2$ *else.*

Proof. • There exists an abelian variety of type $[m, m]$ if and only if $e = 1$ or e is even or $p \not| m$. If it is the case, the corresponding isogeny class contains the product of elliptic curves of trace $-m$ and these curves have $q+1+m \geq 3+1+3 = 7$ rational points, thus at least one rational point of order > 2 (the group of 2-torsion points of an elliptic curve is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). Then, we apply Proposition 14 to conclude that there exists a Prym variety with $(q+1+m)^2$ rational points in this case.

• Else, there does not exist an abelian variety of type $[m, m-1]$ and there exists an abelian variety of type $[m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}]$ if and only if $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$ (since $p|m$ thus $p \not| a_2 = m^2 - m - 1 + 2q$). If it is the case, the corresponding isogeny class contains a Jacobian of dimension 2 (see [6]) which is isomorphic to a Prym variety by Proposition 13.

• Else, using the same arguments as in the first point, we deduce that the product of elliptic curves of trace $-(m-1)$ (such curves exist since $p|m$ hence $p \not| (m-1)$) is isogenous to a Prym variety.

□

Theorem 18. *If $q = p^e$, then $prym_q(2)$ is equal to*

- $(q+1-m)^2$ *if* $e = 1$ *or* e *even or* $p \not| m$
- $(q+1-m+\frac{1+\sqrt{5}}{2})(q+1-m+\frac{1-\sqrt{5}}{2})$ *if* $e \neq 1$, e *odd,* $p|m$ *and* $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$

- $(q+2-m-\sqrt{2})(q+2-m+\sqrt{2})$ *if* $e \neq 1$, e *odd,* $p|m$ *and* $\sqrt{2}-1 \leq \{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2}$
- $(q+2-m)^2$ *else.*

Proof. • There exists an abelian variety of type $[-m,-m]$ if and only if $e=1$ or e is even or $p \not| m$. If it is the case, the corresponding isogeny class contains the product of elliptic curves of trace m. Such elliptic curves have $q+1-m$ rational points, which is greater than or equal to $11+1-6=6$ if $q \geq 11$ and equal to $7+1-5=3$ if $q=7$, thus, in these cases, they must have a rational point of order >2 and Proposition 14 applies. For $q=3,5,9$, we apply Lemma 15.

• Else, there does not exist an abelian variety of type $[-m,-(m-1)]$ and there exists an abelian variety of type $[-m+\frac{1+\sqrt{5}}{2}, -m+\frac{1-\sqrt{5}}{2}]$ if and only if $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$ (since $p|m$ thus $p \not| a_2 = m^2-m-1+2q$). If it is the case, the corresponding isogeny class contains a Jacobian of dimension 2 (see [6]) which is isomorphic to a Prym variety by Proposition 13.

• Else, there does not exist an abelian variety of type $[-m+1+\sqrt{3}, -m+1-\sqrt{3}]$ (since $\{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2} < \sqrt{3}-1$) and there exists an abelian variety of type $[-m+1+\sqrt{2}, -m+1-\sqrt{2}]$ if and only if $\{2\sqrt{q}\} \geq \sqrt{2}-1$ (since $p|m$ hence $p \not| a_2 = m^2-2m-1+2q$). If it is the case, once again, the corresponding isogeny class contains a Jacobian of dimension 2 (see [6]) which is isomorphic to a Prym variety by Proposition 13.

• Else, there does not exist an abelian variety of type $[-m,-(m-2)]$ and the product of elliptic curves of trace $-(m-1)$ (such curves exist since $p|m$ hence $p \not| (m-1)$) is isogenous to a Prym variety as in the first point. □

Remark 19. We can define $N_k(P) = q^k+1+\tau_k(P)$, these are the "virtual numbers of rational points" of P. If $q \leq 9$, then $q+1-2m=-2$ and Theorem 18 asserts that there exists Prym surfaces of type $[-m,-m]$. This gives us examples of Prym varieties with $N_1(P)<0$. In particular, the bounds announced in [1] and proved in [2] on the number of rational points on abelian varieties with nonnegative virtual numbers of rational points do not apply.

References

[1] Y. Aubry, S. Haloui, G. Lachaud. Sur le nombre de points rationnels des variétés abéliennes et des Jacobiennes sur les corps finis. *C. R. Acad. Sci. Paris*, Ser. I 350 (2012) 907-910.

[2] Y. Aubry, S. Haloui, G. Lachaud. On the number of points on abelian and Jacobian varieties over finite fields, to appear in Acta Arithmetica (2013).

[3] A. Beauville. *Prym varieties: a survey.* Proc. symposia in Pure Math. 49 (1989).

[4] N. Bruin. The arithmetic of Prym varieties in genus 3. *Composition Mathematica.* Vol. 144, p. 317-338, 2008.

[5] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenkrper. *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197-272.

[6] E. Howe, E. Nart, C. Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields. *Ann. Inst. Fourrier, Grenoble.* no 59, p. 239-289, 2009.

[7] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28** (1981), no. 3, 721724 (1982).

[8] D. Maisner, E. Nart, appendice de E. W. Howe. Abelian surfaces over finite fields as jacobians. *Experiment. Math.*. Vol 11, p. 321-337, 2002.

[9] D. Mumford. Prym varieties, I *Contributions to Analysis.* (Academic Press, 1974), 325-350.

[10] M. Perret. Number of points of Prym varieties over finite fields. *Glasgow Math. J.*. Vol 48, p. 275-280, 2006.

[11] H. G. Rück. A note on elliptic curves over finite fields. *Math. Comp.*, Vol 49, p. 301-304, 1987.

[12] H. G. Rück. Abelian surfaces and Jacobian varieties over finite fields. *Compositio Math.*, Vol 76, p. 351-366, 1990.
[13] W.C. Waterhouse. Abelian varieties over finite fields. *Ann. Sc. E.N.S.*, (4), 2, 1969, 521-560.

Institut de Mathématiques de Toulon, Université du Sud Toulon-Var and Institut de Mathématiques de Luminy, France
E-mail address: yves.aubry@univ-tln.fr

Department of Mathematics, Technical University of Denmark, Lyngby, Denmark
E-mail address: s.haloui@mat.dtu.dk